National Aeronautics and Space Administration
Jet Propulsion Laboratory, California Institute of Technology

DTN Node Auto-Configuration (DNAC)

Scott Burleigh

Jet Propulsion Laboratory

California Institute of Technology

11 December 2019

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. Government sponsorship acknowledged.

Delay-Tolerant Networking (DTN)

- The DTN architecture is well-defined, tested, and mature.
  - Operational on the International Space Station since 2016.
  - Baselined for Gateway, PACE, and other missions.
  - Already a CCSDS standard, currently being standardized for the Internet by the Internet Engineering Task Force.
- As space flight and other operational environments requiring delay-tolerant networking (undersea, disaster recovery) expand, DTN-based networks will grow in scope and complexity.
- How will DTN scale up to these larger network scenarios?

Current State of the Art (1 of 2)

- End-to-end network traffic is made possible by routing algorithms that determine, given a current network location, which topologically adjacent Bundle Protocol (BP) *node(s)* a BP protocol data unit – *bundle* – must be forwarded to in order to reach its destination.
- These algorithms are computation-intensive, and the computation load increases with the size of the network. A mechanism is needed by which the route calculation performed at any single node can be kept within reasonable bounds even when the network is very large.

Current State of the Art (2 of 2)

- BP nodes must be configured in a number of ways in order to be operational. They need:
  - Knowledge of underlying protocols that provide point-to-point communication capability.
  - Knowledge of network topology, enabling route computation.
  - Knowledge of BP applications' expectations of network service.
  - Knowledge of encryption keys and security policy, enabling secure end-to-end data flow.
- Currently, all such configuration information must be provided by labor-intensive network management. For very large networks, human-managed node configuration will become intractable.

A Possible Way Forward

- *DTN Node Auto-Configuration (DNAC)* can be thought of as very roughly analogous to the Dynamic Host Configuration Protocol (DHCP) of the Internet.
- A new DTN device equipped with DNAC should be able to do all of the following, automatically:
  - Establish the new node's own network identity.
  - Detect its own lower-layer communication resources.
  - Insert itself into the topology of the network.
  - Form pathways for secure communication with its peers.

Supporting Infrastructure (1 of 3)

- A standardized neighbor discovery protocol enables a node to detect the existence of a topologically adjacent node (a *neighbor*), outside of the operation of BP itself.
- One prototype neighbor discovery protocol (IPND) is defined by https://datatracker.ietf.org/doc/draft-irtf-dtnrg-ipnd/.
- Neighbor discovery is based on the periodic broadcast of "beacon" messages over a medium to which all potential neighboring nodes have access, such as an R/F channel. In the course of neighbor discovery, the mutually discovering nodes identify at least one underlying channel by which they may exchange bundles in direct communication.

Supporting Infrastructure (2 of 3)

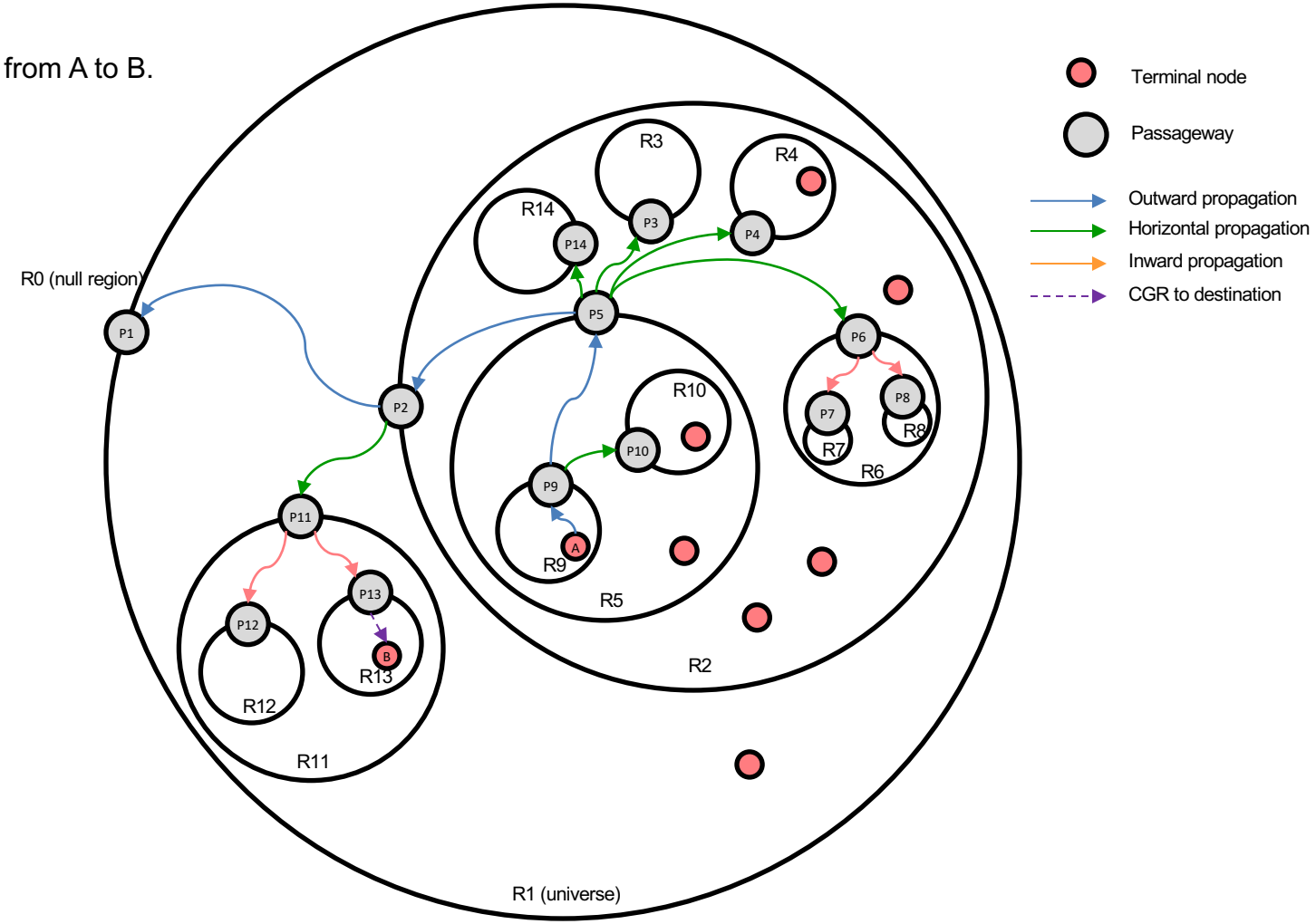
- A standardized delay-tolerant public key infrastructure enables a node to obtain the authenticated public keys of other network nodes and to offer its own authenticated public key to other nodes.
- One prototype delay-tolerant PKI (DTKA) is defined by https://datatracker.ietf.org/doc/draft-burleigh-dtnwg-dtka/.
- DTKA establishes a trusted distributed key authority that multicasts nodes' public keys in messages signed in its own private key. These authenticated public keys can be used to verify signatures attached to bundles that are protected by "bundle integrity blocks" conforming to BP's security protocol.

Supporting Infrastructure (3 of 3)

- A standardized hierarchical grouping system can locate each node within a single, bounded *region* of network topology. Regions are one-for-one with contact plans that declare all anticipated opportunities for direct communication between neighbors, which are used for route computation. When a bundle must be conveyed to a node in a remote region, it is forwarded via designated *passageway* nodes that are able to receive bundles in one region and transmit them within an encompassing – or encompassed – region.
- Hierarchical inter-region routing is a work in progress, but prototypes have been built and tested successfully.

Hierarchical Inter-Region Routing

First bundle sent from A to B.



DNAC Step 1

- First, the new node computes its own unique identifying number.
- Some mechanisms for doing this:
  - It's possible that every node will be running on a device that has an Ethernet interface for communication on its local area network. In this case, the node's unique node number could be some function of the address of that interface.
  - An alternative might be some combination of the current time and the node's location in a relevant coordinate system.

DNAC Step 2

- Next, the new node computes its own public/private key pair.
- The resulting private key is stored locally and is never disclosed to any other entity.
- The corresponding public key will be used by other nodes to verify the signatures on bundles issued by the new node.

DNAC Step 3

- Next, the new node initiates the operation of the neighbor discovery protocol.
- Until it learns otherwise – that is, prior to discovery of its first neighbor – the node considers itself to be the sole occupant of the all-encompassing “universe” region (region number 1).

DNAC Step 4

- The new node discovers its first neighbor, which is termed the new node's *sponsor* node.
- The new node uses the newly identified common underlying communication channel to pass its node number and public key (and possibly other credentials, TBD) to the sponsor node, and vice versa.
- The sponsor node uses some accreditation mechanism, TBD, to determine that the new node will be permitted to join the network, and the new node likewise uses some accreditation mechanism, TBD, to determine that the sponsor node is authentic.

DNAC Step 5

- Upon mutual accreditation, the sponsor node:
  - Informs the new node that its home region is the sponsor node's home region and provides the identity of the passageway node to the home region's encompassing region.
  - Sends the new node a copy of the contact plan for its new home region.
  - Multicasts to all members of the new node's home region a signed contact plan update message, posting a new "registration" contact for the new node, thereby inserting the new node into the contact plan.
  - Multicasts to the network's distributed public key authority a signed public key assertion citing the new node's node number and public key.

DNAC Step 6

- The network's distributed public key authority includes the new node's node number and public key in the next public key announcement bulletin that it multicasts to the network.
- The new node then sends a signed "probe" bundle to node zero. This causes the bundle to be forwarded to nonexistent node zero via Hierarchical Inter-Region Routing, resulting in all passageways in the network discovering the new node's reachability by "backward learning".

Summary

- While mechanisms enabling delay-tolerant networking to scale up to networks of thousands or millions of nodes are non-trivial, they appear to be within reach.
  - Hierarchical inter-regional routing can limit the scope of route computation over contact graphs.
  - Automated node configuration can minimize labor-intensive network management.